Reviewing intelligence, Northern Edge '02.

U.S. Air Force (Adrian Cadiz)

Unity of Effort in Joint Information Operations

By SYNTHIA S. JONES, BERNARD FLOWERS, *and* KARLTON D. JOHNSON

Although information operations have long existed, it was only recently that joint doctrine began including such multidimensional operations in a systematic manner. In addition, the Nation has yet to conduct joint information operations (JIO) utilizing a full range of capabilities—public affairs, civil affairs, psychological operations, operations security, and deception.

Commander Synthia S. Jones, USN, is assigned to the Defense Information Systems Agency; Major Bernard Flowers, USAF, is with the Joint Information Operations Center; and Lieutenant Colonel Karlton D. Johnson, USAF, is serving at Supreme Headquarters Allied Powers Europe.

There is a legal dimension to information operations that is critical to their use. The United States has signed various bilateral and multilateral agreements that affect information operations. As Joint Pub 3-13, *Joint Information Operations*, states: "[information operations] may involve complex legal issues requiring careful review and national-level coordination . . . planners should understand the limitations that may be placed on [campaigns] across the range of military operations." Beyond such statements, however, there is little help for joint planners in maneuvering through the legal maze and even less training available to facilitate this information effort.

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
2002		**00-00-2002 to 00-00-2002**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Unity of Effort in Joint Information Operations	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **National Defense University,300 5th Ave SW, Marshall Hall,Washington,DC,20319-5066**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**6**	

Today there is a perception that the joint community does not exercise this vital segment of the process. In fact, many engagements in which joint information operations have been used were only instances of piecemeal implementation. Current U.S. laws prohibit computer network attack and perception management or limit their use. Thus potent capabilities remain unexploited.

A comparison of the service doctrine with Joint Pub 3-13 reveals that each has considered information operations in terms of its doctrine. FM-100-6, *Army Information Operations*, assumes a land operations perspective—seeking information dominance by tactical advantage on the digital battlefield. Naval Doctrine Pub 6 views information operations in terms of command and control warfare for fleet operations. Even the Air Force, which adopts a more enlightened vision, has an air focus and uses doctrine to control the dimensions of air and space.

The Armed Forces view information operations in terms of the comfortable and the familiar, which is consistent with findings that service efforts fall short of an integrated joint approach.[1] One reason for this lack of integration is oulined in the concept known as *the politicization of strategy*.[2] According to this process, those charged with developing strategic ideas in the services are rarely objective; their job is promoting service interests. This phenomenon is evident in the development of both service and joint information doctrine. The politicization of doctrine means that the services are expert within their domains, and each conceives of doctrine in accordance with its worldview. One effect is that services apply the principles of their military doctrine to information operations. Such operations transcend the traditional boundaries of modern warfare.

services apply the principles of their military doctrine to information operations

The problems of effective joint information operations are compounded by the challenges of coordinating information-centric activities. U.S. Strategic Command is responsible for computer network operations because the preponderance of space-based and computer-centric systems reside within its scope. It also has responsibility for the Joint Information Operations Center at Lackland Air Force Base. However, it would not be appropriate to refer to Commander, Strategic Command, as the commander of information operations, which raises the issue of who is in charge.

Some believe that only combatant commanders could provide the vision, focus, and span of control necessary to protect national infrastructures from information aggression.[3] Moreover, it is argued that joint forces information warfare component commanders are needed to resolve planning problems and execute multifaceted information operations. However, an information operations command structure alone is not the answer. New threats and ubiquitous information technology have changed the limits of information operations. Although joint commanders will play a critical role in information campaigns, a single command does not have the resources, competencies, or partners to meet the enormity of the task. It could have the opposite effect. If one command is responsible for joint information operations, others may defer problems to that command rather than collaborating. Turf wars could erupt if funding becomes associated with particular commanders. In sum, a single command could marginalize the effort and diminish its importance in operational planning. Every combatant commander needs a role in the JIO process, but they are not the only critical players.

Fusing target data, Joint Expeditionary Forces Experiment '00.

U.S. Air Force (Lee E. Rogers)

Involvement on national, state, and local levels as well as in the private sector complicates matters. Attacks using information operations may not be limited to military targets. As identified in Presidential Decision Directive 63, the national infrastructure is a prime target. The attacks on 9/11 proved that the minds of the public are

subject to assault. Consider the crash of the first airliner into the World Trade Center. Few people saw the original impact or caught it on film. But many watched the second plane impact and send a clear message that it was an act of terrorism. The psychological effect was significant: the airline industry nearly went under, stocks plummeted, and Americans were traumatized. It is uncertain whether the Nation immediately realized the second attack was an information operation.

It is also unclear what countermeasures could have minimized the dreadful impact of 9/11. Evidence suggests that there should have been significant collaboration among public and private organizations, the military, media, et al. to deal with the consequences of an attack. But in practice, the Armed Forces have few capabilities available to combat asymmetric attacks on this scale. Both *Joint Vision 2020* and Joint Pub 3-61, *Public Affairs*, encourage commanders to use the media to shape the battlespace, but what relationships and procedures exist to achieve that objective?

if the Nation conducts information operations, the military would not be the only actor on the scene

From a joint perspective, leaders know that information operations are critical to the future. And while there has been an attempt to forge the necessary joint doctrine, something quite different had occurred. The doctrine drafters applied traditional ways of fighting to the JIO strategy. Based on the evidence, this has not been the most effective approach. Tried and true battle strategies will not win future wars fought in the continuum between the human mind and ephemeral cyberspace. Warfare has been transformed in moral, physical, and cybernetic terms. Moreover, technology has radically changed, decreasing the battle rhythm to a matter of seconds rather than days, thereby enabling a degree of influence unknown in the past. The so-called CNN effect reflects this change. Joint warriors must think differently about battlefields, doctrine, and actors.

A New Response

Cyber attacks against the United States by other nations are increasing at an alarming rate. Terrorist groups and foreign governments are using information operations in an effort to level the playing field. Some thirty countries have aggressive offensive information warfare programs, with America as a primary target. To survive such threats, the ways in which information operations are conceived and executed must change.

Representatives of combatant commands and services will come to the table with doctrine on information operations based on their individual worldviews. Effective change will only occur when service doctrine evolves beyond group think and disassociates information operations from service-specific control. Joint leadership must work together to overcome parochial barriers and guide the services towards a more authentic form of joint information operations. Joint Pub 3-13 is a good start, but it is conceptual and not directive in presenting the forms of a synchronized operation. But should joint doctrine provide direction down to service level? That could be a valid concern to the extent that the authority of the combatant commander is infringed. Nevertheless, there must be a better approach to leveraging service competencies. Commanders are the key and must guide their teams to break down service barriers to develop a more appropriate process for the times.

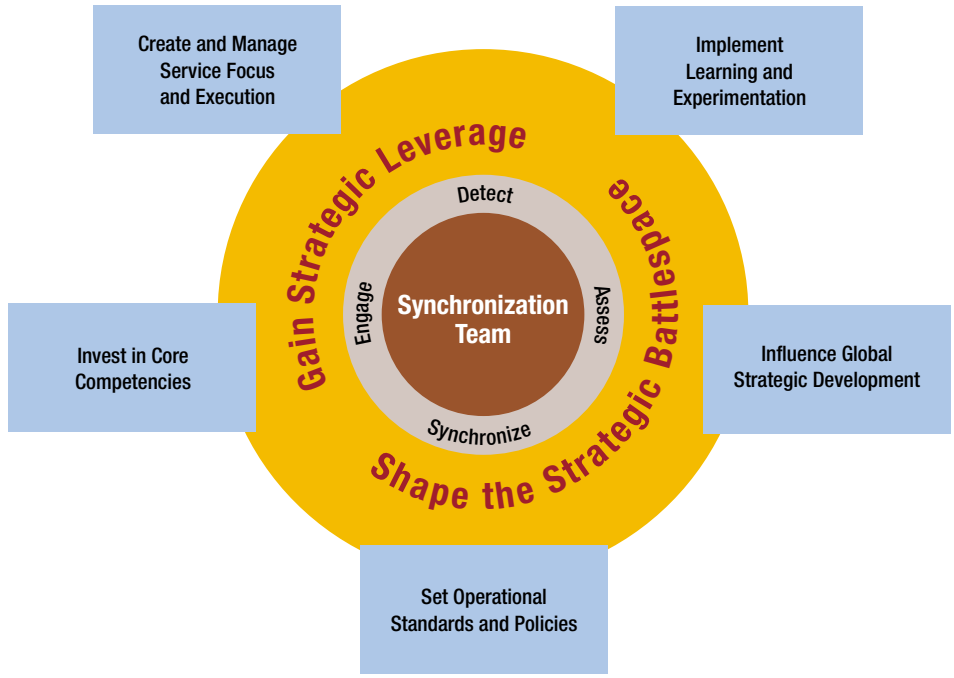
In parallel with the combatant commanders, the joint community should expand its efforts. If the Nation conducts information operations, the military would not be the only actor on the scene. The National Security Agency, Central Intelligence Agency, and other organizations would facilitate activities. Effective operations would also require partnering with the courts to ensure that actions taken are legal as well as capable of withstanding public scrutiny. Links with the media would be needed to provide accurate accounts of events to both domestic and international audiences. By leveraging such relationships, the joint team would be able to design cross-functional responses and thus have a role in influencing the entire operational landscape. These arrangements would provide a more realistic condition for jointness; they could enlarge the team to include stakeholders and employ the full range of natonal capabilities against the threat.

Unity of Effort

Joint information operations need unity of effort. Old models no longer work, and the joint community must reconsider the problem to obtain a workable solution. The information revolution requires an inclusive concept of the various elements of national information power. National security in the information age and the development and exercise of the information component of national strategy require a new paradigm of jointness that incorporates and synchronizes policies and activities in the information realm. Others have also advocated the need for harmonization.

A survey of extant theories and practice suggested the construct for what the authors have called the joint information operations synchronization team (see figure 1). This model also relies on a pioneering study that introduced the concepts of strategic intent, strategic architecture,

Figure 1. Synchronizing Joint Information Operations



and core competency.[4] In redefining strategic success, it emphasized that organizations must shape rather than respond to the future. In the case of information operations, that means fostering a revolution in expertise through the formation of the synchronization team. Appointed by the Secretary of Defense and headed by the Chairman, the team includes representatives of the military, intelligence community, industrial sector, media, et al. The team would accomplish various facets of this model. It would function between the operational and strategic levels to shape campaigns by acquiring and exploiting competitive advantages. Its role would include facilitating defensive information efforts for the joint community, such as detecting information operations, assessing their impact, synchronizing the joint response, and engaging other players. The strength of the team would rest on shaping the strategic information battlespace. While a joint information operations center would interface with the services, the team would develop gateways to other players.

Learning and Experimentation

Current joint doctrine does provide for government-wide exercises. However, key industry players are not included in the scenarios. Knowledge assets, procedures, and plans are not shared with industry or the media; yet the challenge to train as we fight is applicable. All players must be included in the deliberate and crisis action planning process (with consideration for the security of sensitive information) to properly synchronize efforts in the event of an attack. Exercises should be planned and executed jointly and their lessons shared. As teams form the necessary relationships, lines of communication will develop and the United States can shape the future. The knowledge gained will prove invaluable in identifying vulnerabilities across the board: technology, partnerships, competencies, and other factors. Forming these relationships will be the most daunting task.

Global Strategic Development

According to Sun Tzu, the apex of strategy is winning a fight without fighting. The experts have already highlighted cases where other nations are training and planning information operations against the United States. Reacting to the threat is a certain path to failure. Instead, the team must force an enemy into designated killboxes. The team is the focal point for synergizing this effort by shaping information operations,

PSYOP supporting multinational forces, Tradewinds '02.

U.S. Army (Joseph Bonet)

synchronizing community efforts by mapping a strategic architecture, and helping to build that future. A strategic architecture is defined as a "high-level blueprint for the deployment of new functionalities, the acquisition of new competencies (or migration of existing competencies), and the reconfiguring of the interface for those who receive the benefit of said competencies."[5] The joint information operations synchronization team would use this blueprint to influence other nations in the development of tactics, techniques, and procedures for information operations.

shaping the battlespace involves acquiring the right skills and technologies to field a sold information capability

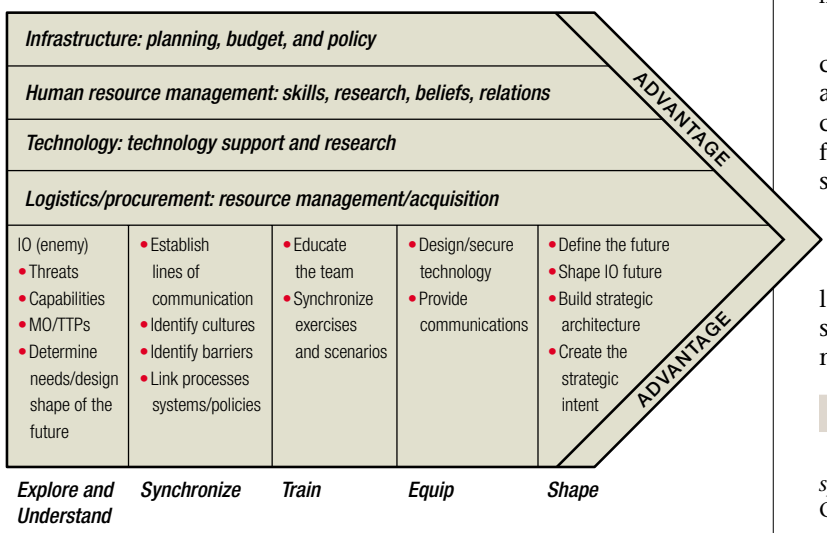
Since the United States is the world leader in technology infrastructure, it has leverage over how others use technology and information concepts. However, that lead is quickly diminishing. During the Persian Gulf War, for example, Iraq used information operations as an asymmetric tool to influence international opinion. America must set the pace and establish the standard. It must also rethink how national security strategy is developed. Chinese strategists have extensively used U.S. doctrine and guidance to formulate their conclusions.[6] The United States can use such documents to guide the rest of the world down its chosen road, simultaneously forging ahead on a different vector. Since perception management is a critical component of information operations, Americans should become experts in global perception management.

Core Competencies

Shaping the battlespace also involves acquiring both the right skills and technologies to field a solid information capability. The joint information operations synchronization team would be responsible for setting the strategic intent of information operations. This intent implies a particular point of view on the long-term environment in which an organization hopes to build a competitive position over time. Considering strategic architecture the brain and strategic intent the heart of the effort implies significant stretch for the team. The intent would then translate into a discussion among the team, learning institutions, and technology firms to determine what core competencies would be needed for the future. These parties would help develop those competencies, matching them to the strategic architecture previously discussed. The result would be a joint effort to secure the intellectual leadership, influence the strategic landscape of the battlespace, and preempt any advantages of use to potential enemies.

Effective joint information operations can be achieved through unity of effort that redefines views of jointness and rethinks the process for shaping the strategic battlespace. Each step in this

Figure 2. Joint Information Operations Value Chain



construct adds layers of improved value to the process, which take the joint information operations synchronization team to higher levels. Based on the work of various consultants and researchers, the JIO value chain can be constructed (see figure 2 above).[7]

The joint information operations synchronization team would affect infrastructure, human resource management, technology, and logistics. These must be harmonized to produce some value that facilitates the effective employment of joint information operations and gains a competitive advantage in this discipline. As the team works through the JIO construct, it will be mindful of the need to establish a competitive advantage and continually strive for enhanced value in every activity. The value chain serves as a visual queue that addresses how an action creates a greater advantage for the United States and whether that value exceeds the real or implied costs of producing it. This aspect of the construct is what separates it from other constructs for information operations.

There are myriad options for the United States with regard to joint information operations. Nonetheless, there are some evident truths:

- information operations will be both a strategic asset and a liability in coming years
- a competitive advantage will be achieved by shaping rather than reacting to the future
- jointness will be expanded to include a larger community of public and private interests working to define core competencies for conducting effective information operations campaigns.

Uniting joint information operations efforts could stimulate discussion so policymakers can attack the problem more effectively. Making complex issues understandable will provide a framework for the questions posed in this analysis. Additionally, taken to its logical conclusion, the construct presented above can address joint and interagency collaboration issues that remain among the most prevalent challenges to information operations. It is time to seek unity of effort in the arena of joint information operations. **JFQ**

NOTES

[1] Randall C. Lane, *Information Operations: A Joint Perspective* (Fort Leavenworth, Kans.: Army Command and General Staff College, 1998).

[2] Stephen M. Walt, "The Search for a Science of Strategy: A Review Essay," *International Security*, vol. 12, no. 1 (Summer 1987), pp. 140–60.

[3] Robert F. Gaines, "Future Information Operations in the Military: Is It Time for a CINC IO?" student paper (Maxwell Air Force Base, Ala.: Air Command and Staff College, April 2000).

[4] Gary Hamel and C.K. Prahalad, *Competing for the Future* (Boston: Harvard Business School Press, 1994).

[5] Ibid.

[6] Qiao Liang and Wang Xiangsui, *Unrestricted Warfare* (Beijing: PLA Literature and Arts Publishing House, 1999).

[7] Michael Porter, *Competitive Advantage: Creating and Sustaining Superior Performance* (New York: The Free Press, 1985) and Michael Porter, *Competitive Strategy: Techniques for Analyzing Industries and Competitors* (New York: The Free Press, 1980). The value chain model was actually developed by McKinsey and Company.

This article is an abridged version of an essay prepared by the authors while attending the Joint Forces Staff College.